Communications of the Association for Information Systems

Volume 28 | Number 1 Article 20

4-1-2011

On Contending with Unruly Neighbors in the Global Village: Viewing Information Systems as Both Weapon and Target

Wm. David Salisbury
Department of MIS, Operations Management, and Decision Sciences, University of Dayton, salisbury@udayton.edu

David W. Miller
Department of Accounting and Information Systems, California State University, Northridge

Lt Col Jason M. Turner
USAF, Department of Aerospace Studies, Indiana University

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 APR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
On Contending with Unruly Neighbors in the Global Village: Viewing Information Systems as Both Weapon and Target	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Indiana University,Department of Aerospace Studies,Indianapolis,IN,46202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**19**	

Communications of the Association for Information Systems

CAIS

On Contending with Unruly Neighbors in the Global Village: Viewing Information Systems as Both Weapon and Target

Wm. David Salisbury

Department of MIS, Operations Management, and Decision Sciences, University of Dayton

salisbury@udayton.edu

David W. Miller

Department of Accounting and Information Systems, California State University, Northridge

Lt Col Jason M. Turner

USAF, Department of Aerospace Studies, Indiana University

Abstract:

While information technologies we employ in business, government, and society have dramatically enhanced our ability to conduct commerce, the vulnerabilities of these systems create potential dangers not often fully apprehended. As an example, criminal and terrorist groups have demonstrated a sophisticated understanding of how to adapt organizational forms and information technologies to advance their agendas, regardless of how contemptible these may be. In this article, we consider how these groups may view information technology and systems both as means by which they may more effectively organize themselves and as potential targets as they subvert the underlying societal assumptions regarding the technology itself. Topics such as these have implications for both IS research and practice because the changing nature of warfare means entities that may have until recently been seen as "non-combatant" are no longer viewed as such; any organization's online resources may be regarded and serviced as legitimate targets. This fact, coupled with the interconnectedness of the global economy, makes it imperative to understand the potential threat—whether this is acted on by criminals, terrorists, or even by hostile nation states—and place greater emphasis on defending vital systems against such attacks.

Keywords: network systems, societal change, political change, conceptual security, computer- and network-enabled crime and terrorism, unconventional warfare

Editor's note: Some of the ideas presented in this article originally appeared in papers presented at the Administrative Sciences Association of Canada Conference.

Volume 28, Article 20, pp. 295-312, April 2011

I. INTRODUCTION

> *Evil is an outreach program. A solitary bad person sitting alone, harboring genocidal thoughts, and wishing he ruled the world is not a problem unless he lives next to us in the trailer park. In the big geopolitical trailer park that is the world today, he does.*
>
> P.J. O'Rourke, *Peace Kills: America's Fun New Imperialism*. New York: Grove Press, 2004, p. 5.

We live in an age of ever-increasing global connectivity and integration, facilitated by the availability of open standards and a robust information infrastructure provided by the Internet [Barabasi, 2002; cf. Zanini and Edwards, 2001]. Open standards and protocols such as TCP/IP, HTML, XML and various file format standards (e.g., Quicken .qfx, Acrobat .pdf, or multimedia formats such as .jpg, .gif, .flv or .mpeg) enable easy communication between enterprises of all stripes, their customers, their suppliers, their competitors, and those organizations that oversee the activities of commerce. This new level of global connectivity has also enabled a variety of knowledge-based and virtual organizational forms to emerge; managers and employees no longer need to be co-located in order to function more or less in unison.

Unfortunately, the very same open standards and robust infrastructure also afford new opportunities for terrorist and criminal organizations that can just as easily leverage this infrastructure as would those who do so for "legitimate" ends. The network is agnostic; it sees no difference between a legal bank deposit, a virus, monies being laundered by a drug cartel, or encoded operating instructions to a terror cell to carry out an operation, so long as a given message lives up to nominal standard network messaging requirements.

This potentially enables criminal and terrorist groups by extending their reach in two ways. First, these groups and individuals have made sophisticated use of information technologies that enable them to organize as knowledge-based virtual organizations, in which technology adoption and use may involve relatively conventional applications (i.e., using technology much as would "legitimate" entities) to enable them to function more effectively in their environments. Second, there is the potential for attack on these enabling systems themselves to steal finances or data or to damage others' systems.

If we set aside, for the moment, understandable indignation at the goals of criminal and terrorist organizations and the means used to achieve them, we discern patterns of use that provide their own clues about why these groups are difficult to restrain and how the global information infrastructure provided by the Internet augments their capabilities and reach. We see innovative uses of information and communication technology often unmatched by the slow-moving institutions that set out to bring them to justice [cf. Castells, 1998]. In addition, by dint of its global connectivity and enabling of the global marketplace, the Internet infrastructure has encouraged many to depend on the capabilities it offers. This dependence means that there are vastly expanded opportunities to steal data or finances. Further, to sever or otherwise compromise access to such capabilities would likely create significant disruption in the everyday lives of millions who depend on network interconnectivity for the monitoring and operation of electrical, telecommunications, and transportation systems [cf. Gorman, 2009], or electronic commerce systems for banking, shopping, and financial trades, to name but a few examples. This state of affairs presents vastly expanded opportunities for unanticipated sorts of activities by criminals, terrorists, and even nation states that never leave the virtual world [cf. Verton, 2003].

The implications of such use and/or targeting go well beyond any localized impact to a single individual, organization, or even nation-state; rather, they represent a deeper threat to the technical and financial infrastructures upon which the modern world depends. Thus, it would seem clear that those charged with defending society; enforcing its laws, and designing, building, and defending systems, as well as those who research how these things are accomplished, may benefit from a review of these possibilities. These roles are not limited to national defense, law enforcement or other government agencies. Any organization with an online presence, regardless of its purpose or affiliation may be a target. Hence, a discussion of the threat from so-called "black hat" entities [cf. Mahmood et al., 2010] is relevant to the private sector as well.

To better understand the possibilities of how technologies may be subverted for nefarious uses, we first draw on a theoretical perspective that provides a language for describing these phenomena. We next describe several examples of how criminal and terrorist organizations have made effective use of existing technologies and technical

infrastructures, both to advance their agendas in more "conventional" ways, and then by extension how these systems themselves have come to be viewed and serviced as targets, both for theft and for disruption. Finally, we describe implications for those who would research the use (and misuse) of information technologies and systems and for those charged with developing and defending them.

II. THE SUBVERSION OF TECHNOLOGIES AND SYSTEMS

For as long as humans have built and deployed technologies and systems, these have been subverted by their own design. Consider an axe used to kill rather than chop wood, a screwdriver to bore holes rather than fasten screws, or, in more contemporary terms, a spreadsheet to write letters rather than manipulate numbers. While technology surfaces in the context of a particular intent, there is almost never a way to effectively circumscribe its uses to its designed purpose alone, although institutional practices such as licensing and prohibition are post hoc attempts to censor the use of a technology or even a technique.

A cursory discussion of the technology creation process illustrates how such subversion occurs. A practice exists which may or may not already utilize some technology, but will almost always involve some technique. The practice is typically a legitimate one, sanctioned or at least tolerated within a particular social milieu. The practice is then built into a technology as a means to facilitate repetitive or consistent use. To the technology's user or its intended beneficiary, the practice and the technology are coextensive; the technology becomes "ready-to-hand" [Heidegger, 1962], an unremarkable background means of continuing the practice. Matters are likely to continue in this way so long as there is no motivation to find other uses for the technology, either by improvement or subversion. But technology, by its very accomplishment of "freezing" practice, circumscribes the actions of larger and larger numbers of people and groups such that the motivation to adapt it to local circumstances and purposes almost invariably creeps in from one angle or another.

To those who have always understood a given technology as belonging unquestionably to one set of practices (e.g., an airplane is meant to enable movement from one location to another, not to be used for political or criminal purposes through hijacking), these unintended adaptations may appear unacceptable and there may emerge a felt need to reclaim the use of the technology in a more acceptable direction. Laws and other societal institutions may be called into play in order to control how the technology is used, or the technology itself may be altered to prevent its use in unanticipated ways. But these actions and alterations are, eventually, only nominal, in that they depend on subversive groups accepting (usually because of the ultimate threat of state force, as Giddens [1987] points out) the jurisdiction of the institutions in question or ignoring the rich potential for alternative uses invariably present within the technologies. Moreover, the number of potential alternative uses is multiplied by the constant drive to refine and extend technologies, either to imbue them with greater functionality (e.g., "smartphones") or to thwart subversions (e.g., anti-virus or firewall software). The ease with which alternative uses can be called into play becomes even greater as technologies are made more general in their purpose.

Interestingly too, just as our processes of refinement attempt to make technologies more useful and less vulnerable to the machinations of those who do not share our cultural and social commitments, once alternative or subversive uses are brought into play, they too become subject to refinement and resistance to our attempts at control (consider how the open-source movement invites processes of refinement from a worldwide public). Consequently, subversive uses themselves become more sophisticated and even institutionalized in their own way. The hijacking of airplanes is a case in point. As controls grew at airports for the purpose of reducing the likelihood of hijacking, means of subverting these controls developed as well. Hijacking continued for a long time to be understood, through its reproduction in scores of instances, by perpetrators and victims alike as a means of diverting the destination of an airplane and using the safety of its passengers as a bargaining tool. This institutionalization of the idea of hijacking, however, was dramatically undermined on September 11, 2001, when hijacked planes were flown into buildings as makeshift cruise missiles rather than safely flown to alternative destinations. Hence, even "illegitimate" uses of our technologies fall into certain patterns which serve to create background expectancies [cf. Garfinkel, 1967] about how they will be used and refined in the future.

One source of language that may be used to describe such unanticipated appropriation of familiar technologies is provided by Giddens [1984] in the form of structuration theory [cf. DeSanctis and Poole, 1992], which focuses on "rules" (normative constraints on action) and "resources" (social objects that enable interaction). As actors engage the world, they do so within available rules and resources, and structure is both imposed on social action and emergent through interaction [Giddens, 1984] [cf. DeSanctis and Poole, 1992; Orlikowski, 1992]. Sewell [1992] elaborates on "rules" as schemata or ideological frameworks that prescribe courses of appropriate action. Sewell suggests that these "recipes for action" are somewhat different from rules in that they may be transposed outside the social sphere in which they were initially generated and internalized. By way of example, e-mail can be seen as having a metaphoric similarity to mailing a pen and paper letter, which might explain its ready adoption—the concept of "mailing" a letter to an "address" was fairly easily transposed to its electronic equivalent once one understood that

both acts involved transferring information, albeit via different media. Resources are cultural products or objects that actors may use to enhance or extend power [cf. Sewell, 1992; Giddens, 1984]. Resource-rich actors are more capable of generating, disseminating, and legitimating schemata among others, although the influence that a resources-rich actor may have is limited by the actor's proximity to those targets of influence, a phenomenon Giddens [1984] terms *time-space distanciation.*

Information technologies, in particular the Internet, may dramatically alter the dynamics of time-space, enabling options for action heretofore not considered. Individuals and groups (even hostile nation states) not previously seen as being able to project power globally are greatly enabled by information and communication technologies, as well as global transportation infrastructures. The increasing ubiquity and mobility of Internet-enabled devices and individualized content delivery mechanisms, such as blogs, tweets, and YouTube™ postings, further boosts the potential that sensational or dramatic acts of terror will in fact prove effective and successful as a means of quickly and inexpensively spreading worldwide awareness and propaganda [Jenkins, 2003]. For example, the 2008 Mumbai terrorist attacks, in particular due to their occurrence near the U.S. Thanksgiving holiday, likely led to greater awareness of them, at least in the U.S. Further, the very dependence of society at large on the global Internet infrastructure also enables attacks that can disrupt seemingly normal activities such as shopping; witness how the 2009 Christmas Eve distributed denial of service (DDOS) attacks against Amazon, Wal-Mart, and others impacted last-minute holiday shopping [Krazit, 2009]. Online banking attacks [e.g., Mills, 2010; Derbyshire, 2010] may diminish confidence even in simple banking transactions.

Concerns about Internet security exist in part because of its very openness. Information systems may be assessed as to confidentiality, integrity, and availability [NIST, 2004], referred to as the CIA triad. While the Internet represents a robust global information system, one needs to recall that it was originally devised with an emphasis on availability (i.e., the network and relevant information should be available to those with legitimate need). Confidentiality (i.e., that a given store of data should only be seen by those with legitimate authority or privilege to do so) and integrity (i.e., data should be changeable only by those with legitimate authority to do so) were not emphasized in the design of the Internet. When the network was exclusively the domain of government, this may have been acceptable. However, with the opening of the infrastructure to the world at large, and given the sensitivity of the data transmitted and criticality of the systems it supports, concerns about these vulnerabilities are now rising to the forefront. Further, the openness of the architecture itself creates vulnerabilities that may lead to denial of availability (e.g., through DDOS attack). When these vulnerabilities come into contact with those who may not share the same beliefs about "appropriate" use and who may have reason to do harm, these concerns become even more salient.

This returns us to the schemata called into play by criminals and terrorists. In most terrorist and criminal organizations, reciprocity and legitimate authority (such as one finds in a market or bureaucratic structure) are necessary; common values and beliefs are also important. However, one of the key appeals is to those who feel a sense of disenfranchisement [Rouleau, 2001]. Religious terrorists, including some white supremacist groups in the United States [Vidal, 2002; Castells, 1998], tend to see themselves as a persecuted minority, victims of violence and/or oppression, and morally justified in any act they undertake against "infidels," "nonbelievers," or "mud people," i.e., anybody who is not one of their kind [Hoffman, 1993] [cf. Stern, 2002]. Legitimate authority in these sorts of groups is derived from shared belief in the cause, or in their cultural identity [Castells, 1998] [cf. Ronfeldt and Arquilla, 2001; Stern, 2002]. Faced with limited resources (at least relative to larger nation states), such groups have historically demonstrated a penchant for creativity in exploiting various technologies to ingenious, albeit nefarious ends [cf. Arquilla and Ronfeldt, 2001], perhaps partly because of their existence outside the mainstream of societies in which these technologies were devised.

Regardless of the perpetrator, traditional defense and law-enforcement entities are unable to defend completely against such threats, in particular in western nations where technology has become so important to daily life (e.g., for banking or shopping). This is because the vast majority of the Internet infrastructure and attached systems in these countries, including privately-owned and managed servers and networks, the telecommunications backbone, and electrical utility grid is privately owned and, therefore, out of the direct control of the government. The inter-connectedness of these systems implies that, should an attack be launched, it could be against (or by employing) a wide range of financial, utility, or other nongovernmental systems to achieve a wide range of potential outcomes. Hence, individuals and organizations that wish to conduct their business by taking advantage of the Internet infrastructure should be aware of such threats and take the appropriate steps to mitigate the risk to which these lead.

Summarizing the discussion thus far, information and communication technologies offer new opportunities for action, some of which may be undertaken by individuals, groups, or nation states with alternative views about what are "acceptable" uses and goals for these technologies. As long as the motivation exists to use the technologies for ends other than originally envisaged, those wishing to circumscribe their use may find themselves fighting a losing

battle. They will be fighting not merely to control such behavior but to put bounds on the creativity of these groups, as well as on the societal causes they choose to support. Such control over those already outside or resistant to our ambit of influence are, at best, extremely difficult to effect.

To address these threats first requires understanding of these groups, their motivations, and their causes, as well as the "occasions for structuring action" [cf. Barley, 1986] afforded by technologies and the resultant organizational forms that have been devised, including their global reach—all of which reveals difficulties in circumscribing the actions by these groups that such technologies enable. In the next section we provide a range of examples that illumine our perspective, and we seek to explain the inherent challenges in restricting both the manner in which these groups can be seen as subverting technologies as well as constraining their *modus operandi*.

III. EXAMPLES THAT ILLUMINE OUR PERSPECTIVE

One upshot of the availability of robust infrastructure and open standards is the emergence of virtual organizational forms based on the sharing and enactment of knowledge [cf. Orlikowski, 2002; DeSanctis and Monge, 1999; Thomas, 2003]. The nature of these organizations means that they are rather malleable, with processes, relationships, and structures among partners changing as shared goals and needs change. The malleability of virtual organizations means that they could form for short periods to achieve specific, shared goals, and then just as rapidly disband. For example, groups that descended on the WTO talks in Seattle in 1999 [de Armond, 2001] represented a diverse agglomeration of labor, anti-globalization, and environmental groups that, while having some elements in common, might also be at cross-purposes on other issues. In a like manner, disparate terror groups could collaborate to launch an attack on an entity regarded as a common enemy.

Criminal and terrorist organizations are generally built around some central organizing theme or set of background expectancies that binds members of the network together [cf. Ouchi, 1980; Maitland, Bryson, and Van de Ven, 1986], and provides a shared interpretative context [cf. Zack, 1993]. Within this context, messages can be readily understood by in-group members that may make no sense to nonmembers (for example, consider a parent attempting to comprehend text messages sent between teenage children and their friends). Members may not be consciously aware of the existence of the knowledge and hence may be unable to communicate it to nonmembers [Bloodgood and Salisbury, 2001]. This common frame of reference makes these groups capable of coordinating without a clear chain of command which could be identified and disrupted—where communication of rich messages is readily accomplished using extremely "lean" media [cf. Lee, 1994; Daft and Lengel, 1986]. Even media as lean as telegraph [cf. Standage, 1998] or more recent limited-bandwidth channels such as Twitter™ could be used by in-group members to communicate quite rich messages using a restricted code. Moreover, the very nature of digital representation and signal manipulation creates unique opportunities to increase the "absolute bandwidth" of otherwise lean media. For example, groups such as al Qaeda are believed to encode messages in graphic files using steganography, with instructions how to access the information sent in brief messages that would be understandable to insiders [Cohen, 2001; Ronfeldt and Arquilla, 2001] [cf. Higgins, Leggett, and Cullison, 2002].

Accordingly, terrorist and criminal groups have demonstrated effectiveness both with codifying knowledge for sharing and creating networks (or perhaps rather, "communities of practice") by applying information technology. With respect to codified knowledge, terrorist groups use a variety of information technologies (e.g., e-mail, CDs, websites) to deliver instructional materials [cf. Arquilla, Ronfeldt, and Zanini, 1999]. Colombian drug cartels have been especially effective in this effort, for example, developing extensive knowledge management systems to map U.S. P-3 Orion surveillance aircraft movements by integrating pilot reports into detailed maps of radar coverage and data mining systems to track telephone calls of their membership, some of whom were killed when the system revealed calls to government officials [cf. Kaihla, 2002]. Further, codified knowledge publicly available online may be used by criminal and terror groups to gather information about potential targets and do reconnaissance from a distance. Google™ Maps "street view" could be a quite effective means to accomplish such efforts. Names and addresses of key law enforcement or defense personnel may also be readily located online or perhaps acquired through technology exploits such as that of the Apple™ iPad in June, 2010 [Tate, 2010] [cf. Ante, 2010].

Recruiting and networking with members are also made easier for terror groups by widespread availability of their message on Internet sites. Although the media in question are extremely lean, the sheer reach of the technical infrastructure across time-space means that individuals who share similar schemata as do those at the head of these organizations, e.g., the sense of disenfranchisement and alienation, will eventually be found and some will likely respond [cf. Schmitt and Lipton, 2010]. Those who do respond can be recruited to places where they can be trained and indoctrinated further, becoming "nodes" in the network that can be eventually activated to perform a particular task using lean, perhaps encoded, messages [cf. Gertz, 2002]. The prevalence and effectiveness of such tactics were revealed during the course of several terror-related investigations including the 2008 arrest of Bryant Neal Vinas, a young American purported to have trained with al Qaeda in the border regions between Afghanistan and Pakistan, and the 2009 arrest of five American citizens in Pakistan. Reports surrounding the arrests attest to the

efficacy of IT-enabled recruitment and command and control tactics such as training and propaganda videos posted and shared on sites such as YouTube™ and coordination via draft comments in shared online e-mail accounts [Harwood, 2009; Robertson and Cruickshank, 2009].

Networking among the membership is important because there is evidence to suggest the most important connections when it comes to accomplishing something that requires connections (e.g., getting a job; getting elements put in place to steal aircraft to demolish a building) are accomplished through so-called "weak" ties [Granovetter, 1973]. The interconnectedness enabled by the Internet takes this "weak ties" perspective to another depth; even members with extremely tenuous links to the organization, but a belief in its message and a willingness to take action on its behalf, can be outfitted and put into action. For example, some have advocated a "cyber-jihad," directed at Israeli government and business websites in particular, but also those of U.S., Indian, Australian, and British interests [USAToday.com, 2002]. In response, Israel has appealed to its citizens to retaliate against Muslim, al Qaeda, and pro-PLO sites [Zanini and Edwards, 2001]. Given the ready availability of hacking tools on the Internet, "script kiddies" (users of scripted hacking procedures) [Fickes, 2003], whether or not linked to any particular group, are easily recruited and require no resources to be expended by the group for which they act. Further, such individuals can act independently of any specific group order, making the identification and, therefore, disruption of any command and control structure difficult.

Ironically, the amorphous state of these groups has largely been driven by their aggressive pursuit by various nation-states (at least those nation-states who do not find such groups useful to promote their own goals). This has forced these groups to evolve into flexible configurations that do not confront their target institutions directly but at their periphery, exploiting overlapping responsibilities and institutional rigidity or by infiltrating the bureaucracy via bribery or extortion [Castells, 1998]. The capacity provided by a robust information infrastructure and open standards enhances the ability to carry out such attacks. The analysis of terrorist groups by Arquilla, Ronfeldt, and Zanini [1999] indicates that a very deadly sort of natural selection is in play: as these groups are systematically surrounded and confronted, they have metamorphosed into different forms using different tactics [cf. Stern, 2003], adopting by necessity the kinds of knowledge-based, virtual organizational forms to which businesses often aspire. The information infrastructure provided by the Internet and the willingness to violate background expectancies about what is and is not appropriate use, offer a wide range of opportunities for action, both in the physical and the virtual realm.

Indeed, when various governments attempt to choke off funding for criminal and terror groups by targeting charitable organizations that tend to serve as fronts for these groups [Lister, 2010], any short-term damage to the ability of terror groups to access funding for their efforts is mitigated by these same terror groups making use of criminal activity to access funding. For example, "phishing," whereby e-mails are sent to unsuspecting Internet users to solicit personal information used to create false identities and/or access bank accounts, or its more sophisticated variant "spear phishing," wherein a targeted e-mail is sent to a potential victim that is part of some group within which a story may be seen as more plausible, are both used to secure funding [FBI, 2009]. Other attacks include "pharming" [Vamosi, 2005] which does not require the user to respond to any e-mail, but simply to attempt to visit a trusted domain for which the address has been corrupted via DNS poisoning [Halley, 2008] and the aforementioned DDOS attack, such as was perpetrated against Amazon.com around Christmas of 2009 [cf. Krazit, 2009]. Another type of attack engages in extortion by launching Trojan horse viruses that infect target machines to encrypt data files on these machines, thereby holding one's data for ransom [Walton, 2005]. While these sorts of attacks have previously been the domain of the small-time hacker, the FBI and other law enforcement organizations suggest the attacks are getting more sophisticated and targeted, indicating organized efforts [Sullivan, 2004], either by criminal and terror groups or by nation-states. More significant examples of so-called "cyber-extortion," either by stealing data and holding it for ransom [cf. Heine and Nussbaum, 2008; Markoff, 2008; Vijayan, 2008] or using the broad reach of the Internet as a threat to disseminate negative information about a target entity [Kravets, 2010], are also now in play. The theft of several million identities from TJX Corporation's TJ Maxx and Marshalls stores in the US and Canada beginning in 2005 (enabled by poor wireless security) is another example of such exploits [cf. Bar On, 2007]. A sophisticated "executive spear-phishing" type attack was used in 2011 to gain access to sensitive data from the Canadian government [Weston, 2011].

Clearly any scheme that enables money to be transported to untraceable locations offers an opportunity for relatively uninterruptible funding for terror and criminal groups and creates difficulties for any effort to track them into nation-states not yet integrated into the global economy [cf. Barnett, 2004]. The amounts are significant; one operation by Ukrainian hackers using the Zeus botnet stole roughly $70 million (US) from the bank accounts of small companies, municipalities, and churches in at least four countries before they were caught [Perez, 2010; cf. Derbyshire, 2010]. In the U.S. $559.7 million (US) in online fraud losses were reported in 2009 [Internet Crime Complaint Center, 2010], more than double the amount in 2008. An FBI survey [Reuters, 2006] indicated that 84 percent of businesses responding suffered a virus attack in the twelve-month period covered by the survey, despite 98 percent of these

same businesses indicating that they employed antivirus software with the average damage resulting from an attack being $24,000 (US). These attacks are also more sophisticated and frequent [Fossi, 2010]; the number of cataloged malicious code signatures increased by 2.9 million (71 percent) between 2008 and 2009 [Symantec, 2010]. The Zeus botnet is representative of this sophistication; the business model developed by its Russian creator features licensing agreements and technical support [Perez, 2010]. The nature of the sorts of virtual attacks we describe here (enabled largely by the design of the Internet) makes them extremely difficult to trace and address. For example, in the FBI survey mentioned above, 44 percent of attacks were traced to China. However, it would be not at all difficult for a hacker based in another country to launch their attack from a poorly defended machine in China or to spoof the address [cf. Tanase, 2003] to make it appear as if the attack came from China.

Further, cyber attacks are not limited to the virtual world alone. Another potential avenue for attack is based on leveraging both the physical and virtual in a coordinated effort. As an example, one could imagine a coordinated attack involving a bombing of a physical site of great importance, coordinated with a simultaneous release of viruses propagated through cell phones or other wireless devices to launch a denial of service attack against emergency communication services [cf. Verton, 2003; Stone, 2009]. The interdependence between critical utility and information infrastructures has gained significant attention with the 2009 release of a theoretical paper regarding the possibilities for creating cascading failures in the U.S. power grid [Markoff and Barboza, 2010]. In 2010, the vulnerability of supervisory control and data acquisition (SCADA) systems such as those used to manage large industrial sites was revealed by the Stuxnet worm, a targeted software that propagated via zero-day exploits in Microsoft Windows [Naraine, 2010] and then attacked an exploit in Siemens' control software that would give control of the target system to an attacker. The threat of such an attack was also vividly demonstrated by the Aurora proof of concept demonstration [AP, 2007] wherein an electrical generator was sent remote commands that caused it to destroy itself. In 2008 concerns were raised that "cyber-extortion" type attacks such as described earlier had already been launched against some utility companies, in essence holding the power grid for ransom [Schachtman, 2008]. Given vulnerabilities of these systems, the movement toward a "smart" electrical grid [cf. US DoE, 2010], which would be even more dependent on information systems and networks, presents yet another concern.

In the virtual world, there are few safe havens online for either side. The "taken for granted" nature of what is and is not anticipated on the Internet has caught terrorist groups themselves flat-footed. Their websites have been found vulnerable to these same kinds of "hack attacks" as soon as they put up an Internet presence; al-Neda was hacked by other groups in 2002, redirecting their links to pornographic sites [Moaveni, 2002]. This demonstrates the flipside of launching online attacks: one tends to live within a "glass house" created by the cycle of hack and counter-hack. In this example, anyone angry at al Qaeda and with access to the Internet could launch denial of service attacks, hack and deface their sites, or engage in any of a variety of other "cyber-attacks" [cf. Denning, 2001]. Despite U.S. government warnings to its citizens against so-called "patriot hacking" [Pace, 2003; Wired, 2003], such an attack was responsible for redirecting requests for Al-Jazeera's home page to a pro-U.S. website in response to the United Arab Emirates network's coverage of the Iraq war in 2003 [Wired, 2003].[1]

Another example of this sort of vulnerability among terror groups is found in the story of a U.S. citizen in Maryland who apparently bought the domain name alneda.com by using the Snapback service to prevent al Qaeda from using it in 2002 (al-Neda, or "the Call," was previously used by al Qaeda) and proceeded to re-post the site, but with added scripts to trace IP addresses of those who posted to the site.[2] He evidently provided this information to the U.S. FBI, but even this example demonstrates the difficulty for large government organizations to respond to these sorts of threats; it seems that by the time somebody at the FBI who understood the significance of what this individual had done was apprised, the original website designer of al Neda posted a warning that the site had been compromised [CNN, 2002; Di Justo, 2002; Schultz, 2002; Hopper, 2002] [cf. Stone, 2005; Robbins, 2002]. Other individuals have engaged in social engineering attacks against potential terrorist targets by infiltrating chat rooms and social networking groups [cf. Hitt, 2007], seeking intelligence that may be passed to law enforcement.

Unfortunately, this lack of comprehension of one's vulnerability online is not limited to terrorist groups; even what would seem relatively secure military devices and systems are not immune to this sort of attack. In December 2009, Shiite insurgents in Iraq purchased off-the-shelf software for approximately $26 (US) that enabled them to hack into and intercept live feeds from U.S. Predator drones, actions which would limit the element of surprise for U.S. attacks and also provide intelligence as to what roads or facilities the U.S. military was monitoring [Gorman, Dreazen, and Cole, 2009]. Details of defense plans shared between the U.S. and South Korea were also apparently hacked in

[1] The U.S. government did (in this case) make good on its threats to punish "patriot hackers," however; the individual plead guilty to charges in 2003 (U.S. Department of Justice, 2003).

[2] A search of the Whois database in January 2011 also suggests that this same entity owns alneda.net, but not alneda.org (i.e., the server and/or owner names appear similar). That this entity also apparently has at times been in business running pornographic websites may somehow seem ironic given the target of its efforts.

November 2009, when a South Korean officer neglected to remove a USB device containing this information from his computer as he switched between a restricted-access website and a site on the open Internet [Kim, 2009]. Both of these incidents reveal problems with management and security controls due to lack of apprehension of the threat.

Finally, it is unclear as to whether some parts of the following example clearly map into either of the "criminal" or "terrorist" categories (depending on legal and political determinations that were not yet settled as of this writing). This said, the November 2010 release of classified U.S. State Department documents by WikiLeaks is interesting for several reasons. First, its leader, Mr. Julian Assange, a product of the "hactivist" culture [cf. Denning, 2001; Khatchadourian, 2010], apparently shares much the same moral clarity as many terrorist groups as to the justness of his cause against the U.S. and other entities he describes as using "... secrecy to conceal unjust behavior" [Chua-Eoan, 2010]. Further, with relatively limited resources, his organization has put a major world power on the defensive [cf. Shane and Lehren, 2010]. We have found limited discussion [Thompson, 2010] regarding either the motivation of U.S. Army Private Bradley Manning, who apparently sent documents to WikiLeaks, or about specific details of his recruitment to Mr. Assange's cause. However, what does seem clear (assuming he is in fact guilty) is that he experienced alienation from U.S. society and the U.S. Army, somehow he learned about the WikiLeaks organization, and he found its mission compelling enough for him to engage in criminal data theft, forsaking an oath of allegiance to his country. This example also offers instruction, not just about the importance of technical defenses, but of procedures to ensure the confidentiality and integrity of data and information in particular [cf. Mehan and Krush, 2009], which we address elsewhere. While the software supporting underlying systems that Private Manning used to steal the data was secure, the Army apparently had not fully implemented the controls where Private Manning was stationed in Iraq. Hence, it was not the technology but its management—a not uncommon failure to implement proper security controls [cf. Fantz, 2010]—that enabled the data theft [cf. Perlow, 2010]. As with the al Neda example above, WikiLeaks was attacked on multiple occasions via DDOS, in one case by a self-described "hactivist for good" with the pseudonym "the Jester" [Greene and Hughes, 2010]. As one might expect, a desire to circumscribe *post hoc* the use of the Internet led U.S. legislators to call for the prosecution of Mr. Assange, with some describing WikiLeaks as a terrorist organization [Epstein, 2010; AP, 2010; Greenemeier, 2010] another applied pressure on Amazon.com™ to drop WikiLeaks content from its servers [Gonsalves, 2010]. The White House issued a no-read order to federal employees [UPI, 2010], and the U.S. Justice Department initiated an investigation of WikiLeaks [Nakashima and Markon, 2010]. WikiLeaks' supporters responded by launching attacks in late 2010 against online resources of businesses that chose to drop it as a customer in response to concerns about its actions, as well against politicians critical of Mr. Assange [Greenemeier, 2010], thus revealing the threats faced by any entity with an online presence.

IV. UNRULY NEIGHBORS—IMPLICATIONS FOR PRACTICE AND RESEARCH

As we have described here, the boundaries of our world are defined to an ever-increasing extent not by geopolitical choice but by the inter-connectedness of our networks [Castells, 1996]. Consequently, terror and criminal groups will be even more likely to draw on available networks and systems to advance their agendas in the future [cf. Arquilla and Ronfeldt, 2001]. We assert that the creativity of terror and criminal groups draws at least in part from their existence outside the mainstream of Western society. This enables them to cast off generally taken-for-granted understandings about "appropriate" uses of information technology and call it into creative use for their own purposes [cf. Arquilla and Ronfeldt, 2001; Castells, 1998; Kaihla, 2002]. Opportunities for unanticipated action abound for those who would make careful study of the information and organizational systems in place and the taken-for-granted understandings surrounding them. Clearly these are concerns for those operating and defending systems.

In terms of IS practice, one example that demonstrates the point we have been trying to make at two levels regards the development of the business of the offshore outsourcing of software development [cf. Lacity, Wilcocks, and Feeney, 1995], and also to open-source development [cf. Open Source Initiative, 2009]. At one level, these phenomena clearly demonstrate the ability of people in locations outside the world's prosperous countries to both understand and contribute to the development of technologies as competently as anyone in the more developed world. However, a second level is that there is often an implicit belief that users in the developing world of technologies that originate in the developed world will use and design the technologies in prescribed and anticipated ways, which may not be consistent with reality. While the cost benefits of offshore software development are well-documented [CNN.com, 2004], the notion that nearly anybody can join al Qaeda or their ilk (as described previously) raises grave concerns for the security of the code that returns to the developed world in terms of possible "back doors" into the software. There is substantial evidence that groups such as al Qaeda see strong linkages between the military might of the West (mainly the United States) and economic might, as well as the heavy dependence on the underlying information technologies and systems that drive such things as B2C or B2B commerce, or even indirectly, military systems [cf. Verton, 2003], so such systems are targets. Accordingly, al Qaeda is known to be recruiting heavily among Muslim students graduating in Computer Science, Computer Engineering, Information Systems, and other IT-related fields [cf. Verton, 2003], and this is a particular concern because anyone could act on

behalf of a criminal or terror group without taking up any resources or without being linked to any part of the core group. A variety of nations, such as Pakistan, Malaysia, China, and Russia, are known sources of various virus and hacking attacks. Some of these attackers may be in it simply for the money or others to advance a cause or country; however, both represent clear threats to computer and information security. Further, global supply chains imply that items such as routers will be more difficult to verify regarding any changes that might make them less secure.

Another implication for practitioners has to do with concerns relevant to single-vendor dominance in the market. Whether it be Microsoft Windows™ or other dominant packages, a lack of "genetic diversity" [Wired.com, 2004] in the software could be seen as leading to vulnerabilities that might not exist otherwise. Further, the advent of "grid" [cf. Gartner, 2004], "utility" [cf. Bhargava and Sundaresan, 2004] or "cloud" computing [cf. Armbrust et al. 2010], which implies even tighter integration among disparate systems around the world, would present a tempting target to a motivated, intelligent, and resourceful group. The decentralization of computing capabilities and data storage inherent in such architectures could present a situation in which wholesale disruption of the Internet infrastructure is unnecessary; an attacker would simply need to degrade the portion of the grid responsible for targeted services, while leaving other circuits and connections open for command and control.

As a response to the possibilities we raise here, the growing concern about information and network security has led to a veritable plethora of certificate programs in information assurance, network security, and related areas. For example, the lead author of this article is involved in the development of a cyber-security course sequence at his university to produce professionals for government and industry. Standards that emphasize the systematic assessment of and defense against threats to information security have been promulgated by government agencies, for example, National Institute of Standards and Technology (NIST), Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), and Federal Information Security Management Act of 2002 (FISMA), as well as private entities such as the Committee for Sponsoring Organizations of the Treadway Commission (COSO) and Control Objectives for Information and related Technology (COBIT).

Each of the standards and processes mentioned above emphasizes systematic efforts to identify information systems and assets as to their criticality, including the value of the information and potential damage if the confidentiality, integrity or availability of the system or asset were compromised. This process would ideally be followed by an assessment of vulnerabilities that may exist to these assets (e.g., known Windows exploits if one is running Windows-based systems) potential threats (i.e. criminals might want to steal customer data) and how these might be mitigated (e.g., creating a systematic regime by which "patch Tuesday" or other updates from Microsoft are distributed and installed to all PCs). This said, most of the mandated standards above deal with government-owned and managed systems or systems used in industries with significant government regulatory oversight (e.g., hospitals working under the Health Insurance Portability and Accountability Act of 1996). The vast majority of privately-owned systems are under no such mandates to enhance security, however. Though there are ample motivations for private entities to safeguard their systems (e.g., the threat of legal action if sensitive data is lost, or the effort that recovery from an attack would entail), in 2009 less than half of corporations surveyed used external security audits at least once per year, though this was an increase from the previous year [PRNewswire, 2010]; another survey suggests half of small business owners believe the cost of robust security outweighs the benefit despite concerns that such organizations are being explicitly targeted [National Cyber Security Alliance, 2010]. Further, nearly every major federal agency suffered information security failures in 2009 [U.S. Government Accountability Office, 2010]. Such findings are especially troubling because the interrelated nature of systems and infrastructures could well lead to shared risks that are not well understood. Imagine, as an example, a major military base that depends on a local utility for its electrical power. Are the defenses in place at the utility provider commensurate with the risk to a national defense asset?

That this awareness has arisen leads to an emphasis on the importance of information systems/technology management and governance, as defense against such threats as we describe here are not strictly of a technical nature. Software vendors can (and do) offer a range of patches, updates, and the like to their customers, but if there is no effective means by which such fixes are consistently and routinely applied throughout the organization, the effort at developing these protections is for naught. In a reality in which any point of access is also a potential point for exploit, effective management and governance of the IT security function are critical. The critical element in any systematized attempt to create an information assurance regime is individuals engaged in this process who can effectively assess threats, defenses, and risks, as well as the costs and benefits of various mitigation strategies; simply following procedures will not be enough. As one example, security audits must no longer be thought of as something to be dispensed with and then left lying fallow until the next audit; managers will by necessity need to view security as an ongoing risk-management effort, continually adjusting and improving to address emergent vulnerabilities and threats.

In the presence of well-trained, skilled, and motivated attackers, every aspect of system defense will likely need rethought. For example, the current means by which many organizations secure their systems is to purchase the latest updates from Symantec®, McAffee®, or Kaspersky® (among several others), which are traditionally based on viruses characterized by specific signatures that can be identified [cf. Shipley, 2010]. However, the advent of threats, such as polymorphic viruses [cf. Grimes, 2007], packed viruses, targeted viruses, crimeware toolkits [cf. Mills, 2010; Perez, 2010] and the sheer volume of new viruses represent threats against which signature-based antivirus software is not well-equipped to defend [cf. Shipley, 2010]. Hence, defenses will have to adjust; one such adjustment is the Tripwire™ software [cf. Fioretti, 2006], which makes use of a hashing algorithm to keep track of any changes to files on a given server or workstation. Another is Bouncer™ from Coretrace [Grimes, 2009], which involves the use of application white-listing rather than signature-based defenses to protect against malware.

While we do not engage deeply in the notion of nation-state sponsored effort here, it is worthwhile to note that nation-states also bring unique schemata to their understanding of information technologies and their uses; indeed, one need only consider some lessons learned about IT in the wake of the 1990-1991 Persian Gulf War. Specifically, the same types of command and control technologies and communications networks that were key enablers for the US-led coalition proved to be strategic liabilities for the Iraqi leadership and command authority once these were selectively targeted and destroyed during the air campaign. The resulting "strategic paralysis" of the Iraqi military, despite its nearly overwhelming numbers of conventional ground forces, was caused by Iraq's dependence on a sophisticated and integrated IT infrastructure that had been rendered ineffective [Warden, 1994], which illustrates the kinds of IT-centric liabilities and vulnerabilities with which most any modern nation-state must contend. Since that time China, Russia, Israel, and the United States (to name a few) have engaged in systematic efforts to identify and exploit weaknesses in IT systems and to develop IT-centric target sets in the event of a "cyber-war" [cf. Clark and Knake, 2010]. For example, an Israeli raid on a Syrian radar site in 2007 was preceded by a cyber attack to disable Syrian defenses [cf. Clark and Knake, 2010]. Indeed, it is plausible that the more sophisticated extant malware is state-sponsored [cf. Broad, Markoff and Sanger, 2011] and perhaps earlier, less targeted attacks served as a "proof of concept" [Garfinkel, 2003]; there is evidence that the Stuxnet worm of 2010 has at least some characteristics in common with the earlier Conficker worm [Acohido, 2011]. In addition, these nation-states are also considering what may previously have been seen as nonmilitary targets (e.g., banks or civilian power generation); the Russian invasion of Georgia in 2008 was preceded by a cyber-attack that crippled Georgian defenses [Markoff, 2008] and also targeted banks and other nonmilitary sites [cf. Clarke and Knake, 2010].

Just as there are a variety of implications for various groups who have interest in the development, use, and defense of information systems, there are a variety of potential avenues of study for IS researchers. We suggest that the examples provided here illustrate novel uses and appropriations of information technology to enable knowledge-based virtual organizations that can be applied in a variety of domains, including terrorist and criminal organizations. This evidence shows that such groups appropriate technology as a means to organize their various nefarious activities and target those same technologies as well. Certainly, research aimed at increasing our understanding of how terrorist and criminal organizations appropriate information technology to disreputable ends would prove valuable. Yet, we have found only one research article [Cesera, 2005] that has specifically studied information technology appropriation by terrorist organizations, finding a progressively wider adoption of goods and services related to the technology. The many other scholarly articles that examine terrorist and criminal organizations and information technology use have concentrated on issues of counter-terrorism or counter-criminal measures. While not diminishing the importance of these defensive measures, we attempt to point out that it is equally important (arguably, perhaps more important) to understand the deeper social structures involved in information technology appropriation by such groups. This knowledge would aid anti-terrorism and anti-criminal efforts as they develop or even provide some predictive power of the behaviors of such groups to thwart their efforts.

One particularly interesting avenue for study would be to investigate in depth the suggested relationship between disenfranchisement and innovative or unique appropriation of technologies. Another possible direction might be to investigate more carefully how nation-states can adopt the novel institutional changes suggested here and thereby resist this direct challenge to their sovereignty and legitimacy [cf. Castells, 1996; 1998]. Further investigation as to what "knowledge" is and how it can be best "managed" is also indicated; clear understandings in this area would offer the benefit of better understanding how criminal and terrorist groups operate and also how nation-states and legitimate enterprises might arrange their resources in a more effective manner. Likewise, research into alternative forms of organization that focus more on building norms and shared beliefs within an organization rather than focusing solely on command and control hierarchies [cf. Maitland, Bryson and Van de Ven, 1986; Ouchi, 1980] may also be fruitful pursuits for further study. Similarly, organizations described here possess attributes typical of lean organizations [cf. Jenner, 1998]; for example, they are able to assemble and maintain dispersed organizational structures with minimal expense of organizational resources. Consequently, study of the means by which such organizations ally and collaborate to achieve their goals with extremely lean organizational structures can illuminate

effective means through which organizations, large and small, as well as individuals in the global marketplace can connect and collaborate to legitimate ends.

V. CONCLUSION

Plainly there are groups and individuals that do not share the cultural assumptions and trajectories of the societies from which the technologies they use originate, who have, nevertheless, achieved a level of technical and organizational sophistication that makes them resourceful and dangerous adversaries to any nation-state or organization they may choose to target. Because we blind ourselves to the alternative possibilities afforded by or contained within our technologies, we disarm ourselves. That our technologies have become "ready-to-hand" closes us to understanding their use in creative ways, and we ignore the deeper issues in our world that these subversive uses of technology mask; for one, that "targets" in "warfare" are no longer necessarily military or government resources, and for another, are no longer only at the boundaries between ourselves and those who may wish us ill.

The reality of technological asymmetry is an indicator of the structurational nature of our primary argument; that information technology serves both as a means of enabling criminal and terrorist action and as a potential target of such action. In particular, those nations in which such technology is embedded and pervades nearly every aspect of economic infrastructure and provision of human services are, in fact, most vulnerable and sensitive to any disruptions or degradation of such infrastructure; such technological dependence affords more opportunities to affect greater disruptions by smaller and smaller groups [Jenkins, 2003]. However, it is precisely the pervasiveness, reach, open standards, and low marginal cost of acquisition of such technologies that enable the creative, geographically dispersed, and unexpected uses of such technology for illegitimate ends.

History has shown that those people who are at times dismissed by the more technologically advanced (and, therefore, technologically dependent) world have made careful study of systems, technology, and procedures at work in the developed world and actively seek to exploit their weaknesses. These threats will exist so long as commerce and communication are online, and defense will require ever-increasing sophistication and vigilance. However, mechanisms do exist to identify information assets, assess threats against them, and mitigate the associated risk. This would seem the most appropriate response, and to the extent that this article has raised awareness that leads to action on the part of both government agencies and private enterprise to enhance technical defenses and human capital directed toward this end [cf. Nakashima and Krebs, 2009], we believe our effort here has served its purpose.

ACKNOWLEDGMENTS

The authors wish to express their gratitude to Abhijit Gopal, who was instrumental getting earlier versions of these ideas brought forth, and whose encouragement to continue the work has aided the development of this article.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Acohido, B. (2011) "Why the Stuxnet Worm Could be Conficker's Cousin", *USA Today*, Jan. 19, http://content.usatoday.com/communities/technologylive/post/2011/01/why-the-stuxnet-worm-could-be-conficker-cousin-/1 (current March 1, 2011).

Ante, S.E. (2010) "Dark Side Arises for Phone Apps: Security Concerns Prompt Warnings", *Wall Street Journal* (June 3), pp. B1-2.

Armbrust, M. et al. (2010) "A View of Cloud Computing", *Communications of the ACM* (53)4, pp. 50–58.

Arquilla, J. and D. Ronfeldt (2001) "Afterword: The Sharpening Fight for the Future" in Arquilla, J. and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy* (Sept.), Santa Monica, CA: Rand, pp. 363–371.

Arquilla, J., D. Ronfeldt, and M. Zanini (1999) "Networks, Netwar, and Information-Age Terrorism" in Lesser, I.O. et al. (eds.) *Countering the New Terrorism*, Rand Paper MR-989-AF, Santa Monica, CA: Rand, pp. 39–84.

Associated Press (2007) "Video Shows Hacker Attack On Power Grid: Simulated Cyber Attack Details Potential Damage to U.S. Electrical System", *CBSNews.com*, Sep. 27, http://www.cbsnews.com/stories/2007/09/27/tech/main3303616.shtml (current Mar. 3, 2011).

Associated Press (2010) "McConnell: WikiLeaks Chief 'A High-Tech Terrorist'" *CBSNews.com*, Dec. 5, http://www.cbsnews.com/stories/2010/12/05/ap/congress/main7119787.shtml (current Jan.14, 2011).

Bar On, S. (Producer) (2007) *60 Minutes: High Tech Heist* (television broadcast), Washington, DC: CBS News, Nov. 25.

Barabasi, A. (2002) *Linked: The New Science of Networks*, Cambridge, MA: Perseus Publishing.

Barley, S.R. (1986) "Technology as an Occasion for Structuring: Evidence from Observation of CT Scanners and the Social Order of Radiology Departments", *Administrative Science Quarterly* (31), pp. 78–108.

Barnett, T.P.M. (2004) *The Pentagon's New Map: War and Peace in the Twenty-First Century,* New York, NY: Putnam.

Bhargava, H. and S. Sundaresan (2004) "Computing as Utility: Managing Availability, Commitment, and Pricing Through Contingent Bid Auctions", *Journal of Management Information Systems* (21)2, pp. 201–227.

Bloodgood, J.M. and W.D. Salisbury (2001) "Understanding the Influence of Organizational Change Strategies on Information Technology and Knowledge Management Strategies", *Decision Support Systems* (31)1, pp. 55–69.

Broad, W. J., Markoff, J. and Sanger, D. E. (2011) "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *New York Times,* Jan. 16, p. A1.

Castells, M. (1996) *The Information Age: Economy, Society and Culture, Vol. 1, The Rise of the Network Society*, Malden, MA: Blackwell.

Castells, M. (1998) *The Information Age: Economy, Society and Culture, Vol. 3, The End of Millennium*, Malden, MA: Blackwell.

Ceresa, A. (2005) "The Impact of 'New Technology' on the 'Red Brigades' Italian Terrorist Organization", *European Journal on Criminal Policy and Research* (11), pp. 193–222.

Chua-Eoan, H. (2010) "WikiLeaks Founder Julian Assange Tells *Time*: Hillary Clinton 'Should Resign'", *Time*, Nov. 30, http://www.time.com/time/nation/article/0,8599,2033771,00.html (current Jan. 14, 2011).

Clark, R.A. and R.K. Knake (2010) *Cyberwar: The Next Threat to National Security and What to Do About It*, New York, NY: HarperCollins.

CNN.com (2002) "Pornographer Says He Hacked al Qaeda", Aug. 8, http://archives.cnn.com/2002/US/08/08/porn.patriot (current Jan. 14, 2011).

CNN.com (2004) "IBM Giveth, Taketh Away: WSJ: Internal Documents Say Millions of Dollars to be Saved by Moving Thousands of Jobs Overseas", Jan. 19, http://money.cnn.com/2004/01/19/news/companies/ibm/, (current Feb. 24, 2011).

CNN.com (2008) "Third Undersea Internet Cable Cut in Mideast", Feb. 1, http://www.cnn.com/2008/WORLD/meast/02/01/internet.outage/ (current Jan. 11, 2011).

Cohen, A. (2001) "When Terror Hides Online", *Time* (158)21, p. 65.

Daft, R.L. and R.H. Lengel (1986) "Organizational Information Requirements, Media Richness and Structural Determinants", *Management Science* (32)5, pp. 554–571.

de Armond, P. (2001) "Netwar in the Emerald City: WTO Protest Strategy and Tactics" in Arquilla, J. and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy,* Santa Monica, CA: Rand: pp. 201–235.

Denning, D. (2001) "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" in Arquilla, J. and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica, CA: Rand: pp. 239–288.

Derbyshire, D. (2010) "Thousands of Online Banking Customers Have Accounts Emptied by 'Most Dangerous Trojan Virus Ever Created'" *Daily Mail Online*, Aug. 11, http://www.dailymail.co.uk/sciencetech/article-1302062/New-trojan-virus-Zeus-v3-empties-online-bank-accounts.html# (current Jan. 12, 2011).

DeSanctis, G. and P. Monge (1999) "Communication Processes for Virtual Organizations", *Organization Science* (10)6, pp. 693–703.

DeSanctis, G. and M.S. Poole (1994) "Capturing the Complexity of Advanced Technology Use: Adaptive Structuration Theory", *Organization Science* (5)2, pp. 121–147.

Di Justo, P. (2002) "How al Qaeda Site Was Hijacked", *Wired,* Aug. 10, http://www.wired.com/culture/lifestyle/news/2002/08/54455 (current Jan. 14, 2011).

Epstein, J. (2010) "Rep. Peter King: Prosecute WikiLeaks, Julian Assange", *Politico,* Nov. 29, http://www.politico.com/news/stories/1110/45667.html (current Jan. 14, 2011).

Fantz, A. (2010) "Expert: Pentagon Cybersecurity Changes 'Very Basic,' Very Late", *CNN.com,* Dec. 2, http://www.cnn.com/2010/US/12/02/wikileaks.computer.security/index.html (current Jan. 14, 2011).

FBI (2009) "Spear Fishers: Angling to Steal Your Financial Info", Apr. 1, http://www.fbi.gov/page2/april09/spearphishing_040109.html (current Jan. 14, 2011).

Fickes, D. (2003) "Beware of Script Kiddies", *Government Security*, May 1, http://govtsecurity.com/mag/beware_script_kiddies/ (current Jan. 14, 2011).

Fioretti, M. (2006) "How to Set up and Use Tripwire", *Linux Journal,* Apr. 28, http://www.linuxjournal.com/article/8758 (current Jan. 14, 2011).

Fossi, M. (2010) "Online Threats: What Governments Need to Know", *Summit* (13)7, Nov., pp. 15–16.

Garfinkel, H. (1964) "Studies of the Routine Grounds of Everyday Activities", *Social Problems* (11)3, pp. 225–250.

Garfinkel, S. (2003) "Proof of Concept",.*Technology Review* (106)4, p. 28.

Gartner, J. (2004) "Grids Unleash the Power of Many", *Technology Review,* Jan. 14, http://www.technologyreview.com/articles/05/01/wo/wo_gartner011405.asp?p=0 (current Jan. 14, 2011).

Gertz, B. (2002) "Terror Cells at Liberty to Strike", *The Washington Times,* Sept. 18, p. A01.

Giddens, A. (1984) *The Constitution of Society*, Los Angeles, CA: University of California Press.

Giddens, A. (1987) *The Nation State and Violence*, Los Angeles, CA: University of California Press.

Gonsalves, A. (2010) "Amazon Ousts Wikileaks", *InformationWeek,* Dec. 2, http://www.informationweek.com/news/software/web_services/showArticle.jhtml?articleID=228500114 (current Jan. 14, 2011).

Gorman, S. (2009) "Electricity Grid in U.S. Penetrated By Spies", *Wall Street Journal,* Apr. 8, http://online.wsj.com/article/SB123914805204099085.html (current Jan. 14, 2011).

Gorman, S., Y.J. Dreazen, and A. Cole (2009) "Insurgents Hack U.S. Drones", *Wall Street Journal,* Dec. 17, http://online.wsj.com/article/SB126102247889095011.html (current Jan. 14, 2011).

Granovetter, M.S. (1973) "The Strength of Weak Ties", *American Journal of Sociology* (78)6, pp. 1360–1380.

Greene, R.A. and N. Hughes (2010) "'Hacktivist for Good' Claims WikiLeaks Takedown", *CNN.com,* Nov. 29, http://articles.cnn.com/2010-11-29/us/wikileaks.hacker_1_wikileaks-computer-hacker-cyber-attack?_s=PM:US (current Jan. 14, 2011).

Greenemeier, L. (2010) "WikiLeaks Supporters Attack Web Sites of MasterCard and Other Opponents", *Scientific American,* Dec. 8, http://www.scientificamerican.com/blog/post.cfm?id=wikileaks-supporters-attack-web-sit-2010-12-08 (current Jan. 11, 2011).

Grimes, R.A. (2007) "Stopping Malware That Mutates on Demand", *Infoworld,* Oct. 26, http://www.infoworld.com/d/security-central/stopping-malware-mutates-demand-384 (current Jan. 14, 2011).

Grimes, R.A. (2009) "Application Whitelisting Review: CoreTrace Bouncer", *Infoworld,* Nov. 4, http://www.infoworld.com/d/security-central/application-whitelisting-review-coretrace-bouncer-600 (current Jan. 14, 2011).

Halley, B. (2008) "How DNS Cache Poisoning Works", *NetworkWorld,* Oct. 20, http://www.networkworld.com/slideshows/2008/102008-dns-and-cache-poisoning.html (current Jan. 14, 2011).

Harwood, M. (2009) "Five Muslim Americans Arrested in Pakistan; Believed to Want to Wage Jihad", *Security Management,* Dec. 10, http://www.securitymanagement.com/news/5-muslim-americans-arrested-pakistan-believed-want-wage-jihad-006542 (current Jan. 14, 2011).

Heidegger, M. (1962) *Being and Time*, San Francisco, CA: Harper.

Higgins, A., K. Leggett, and A. Cullison (2002) "How al Qaeda Put Internet in Service of Global Jihad", *Wall Street Journal* (240)94, Nov. 11, p. A1.

Hitt, J. (2007) "Behind Enemy Lines with a Suburban Counterterrorist", *Wired*, Oct. 23 http://www.wired.com/politics/security/magazine/15-11/ff_rossmiller (current Jan. 14, 2011).

Hoffman, B. (1993) *"Holy Terror": The Implications of Terrorism Motivated by a Religious Imperative*. Rand Paper P-7834, Santa Monica, CA: Rand.

Hopper, D.I. (2002) "Man Hijacks al Qaeda Web Site", *Global Security,* July 30, http://www.globalsecurity.org/org/news/2002/020730-net1.htm (current Jan. 14, 2011).

Internet Crime Complaint Center (2010) *2009 Internet Crime Report,* http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf (current Jan. 14, 2011).

Jenkins, B.M. (2003) "International Terrorism" in Art, R.J. and K.N. Waltzpp (eds.) *The Use of Force: Military Power and International Politics*, Blue Ridge Summit, PA: Rowman & Littlefield, pp. 77–84.

Jenner, R.A. (1998) "Dissipative Enterprises, Chaos, and the Principles of Lean Organizations", *Omega, International Journal of Management Science* (26)3, pp. 397–407.

Kaihla, P. (2001) "Weapons of the Secret War", *Business 2.0* (2)9, Nov., pp. 98–101.

Kaihla, P. (2002) "The Technology Secrets of Cocaine Inc.", *Business 2.0* (3)4, July, pp. 74–80.

Khatchadourian, R. (2010) "No Secrets: Julian Assange's Mission for Total Transparency", *The New Yorker,* June 7, http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian (current Jan. 14, 2011).

Kim, K.T. (2009) "Hackers Steal S. Korean-US Military Secrets", *The China Post,* Dec. 18, http://www.chinapost.com.tw/asia/korea/2009/12/18/237102/Hackers-steal.htm (current Jan. 14, 2011).

Krazit, T. (2009) "DDoS Attack Hobbles Sites, Including Amazon", *Cnet.com,* Dec. 23, http://news.cnet.com/8301-30684_3-10421577-265.html (current Jan. 14, 2011).

Lacity, M.C., L.P. Wilcocks, and D.F. Feeney (1995) "IT Outsourcing: Maximize Flexibility and Control", *Harvard Business Review* (73)3, pp. 84–93.

Lee, A.S. (1994) "Electronic Mail as a Medium for Rich Communication: An Empirical Investigation Using Hermeneutic Interpretation", *Management Information Systems Quarterly* (18)2, pp. 143–157.

Lister, T. (2010) "Security Brief: The 'Urgent' Choking of al Qaeda's Money Supply", *CNN.com,* May 12, http://news.blogs.cnn.com/2010/05/12/security-brief-the-urgent-choking-of-al-qaedas-money-supply (current Jan. 14, 2011).

Mahmood, M.A. et al. (2010) "Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue", *Management Information Systems Quarterly* (34)3, pp. 431–433.

Maitland, I., J. Bryson, and A. Van de Ven (1986) "Sociologists, Economists, and Opportunism", *Academy of Management Review* (10)1, pp. 59–65.

Markoff, J. (2008) "Before the Gunfire, Cyberattacks", *New York Times,* Aug. 13, p. A1.

Markoff, J. and D. Barboza (2010) "Academic Paper in China Sets off Alarms in U.S.", *New York Times,* Mar. 20, p. A10.

Martinez-Cabrera, A. (2009) "Hackers' Attacks Rise in Volume Sophistication", *SFGate.com,* Dec. 26, http://articles.sfgate.com/2009-12-26/business/17461266_1_hackers-criminals-security-firm (current Jan. 14, 2011).

Mehan, J.E. and W. Krush (2009) *The Definitive Guide to the C&A Transformation,* Cambridgeshire, UK: IT Governance Publishing.

Mills, E. (2010) "Zeus Trojan Steals $1 Million from U.K. Bank Accounts", *Cnet.com,* Aug. 10, http://news.cnet.com/8301-27080_3-20013246-245.html (current Jan. 14, 2011).

Moaveni, A. (2002) "Bin Laden Hacked!" *Time,* July 31, http://www.time.com/time/world/article/0,8599,332914,00.html (current Jan. 14, 2011).

Nakashima, E. and B. Krebs (2009) "As Attacks Increase, U.S. Struggles to Recruit Computer Security Experts", *The Washington Post,* Dec. 23, p. A01.

Nakashima, E. and J. Markon, (2010) "WikiLeaks Founder Could Be Charged Under Espionage Act", *Washington Post,* Nov. 30, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112905973.html (current Jan. 14, 2011).

National Cyber Security Alliance (2010) "Small Businesses Do Not See Themselves as Cybercrime Targets", Nov. 30, http://staysafeonline.mediaroom.com/index.php?s=43&item=72 (current Jan. 12, 2011).

National Institute of Standards and Technology (2004) "Standards for Security Categorization of Federal Information and Information Systems", Feb., http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (current Jan. 14, 2011).

O'Rourke, P.J. (2004) *Peace Kills: America's Fun New Imperialism,* New York, NY: Grove Press.

Orlikowski, W.J. (1992) "The Duality of Technology: Rethinking the Concept of Technology in Organizations", *Organization Science* (3)3, pp. 398–427.

Orlikowski, W.J. (2002) "Knowing in Practice: Enacting a Collective Capability in Distributed Organizing", *Organization Science* (13)3, pp. 249–273.

Ouchi, W.G. (1980) "Markets, Bureaucracies, and Clans", *Administrative Science Quarterly*, pp. 129–141.

Pace, D. (2003) "Government Warns 'Patriot Hackers,'" *CRN.com,* Feb. 12, http://www.crn.com/security/18821779 (current Jan. 14, 2011).

Perez, E. (2010) "Hackers Siphoned $70 Million", *Wall Street Journal,* Oct. 2, http://online.wsj.com/article/SB10001424052748704029304575526393770024452.html (current Jan. 13, 2011).

Perlow, J. (2010) "WikiLeaks: How Our Government IT Failed Us", *ZD.net,* Dec. 1, http://www.zdnet.com/blog/perlow/wikileaks-how-our-government-it-failed-us/14988 (current Jan. 14, 2011).

Poole, M. and G. DeSanctis (1992) "Understanding the Use of Group Decision Support Systems: The Theory of Adaptive Structuration" in Fulk, J. and C. Steinfield (eds.) *Organizations and Communication Technology*, Newbury Park, CA: Sage, pp. 173–193.

PR Newswire (2010) *Sixth Annual IT Security Survey: 45% of Enterprises Employ Outside Security Audits at Least Once a Year, a Ten Percentage Point Increase Over Previous Year,* Oct. 12, http://www.prnewswire.com/news-releases/sixth-annual-it-security-survey-45-of-enterprises-employ-outside-security-audits-at-least-once-a-year-a-ten-percentage-point-increase-over-previous-year-104777724.html (current Jan. 13, 2011).

Reuters (2006) "Online Attacks Common for Businesses—FBI", Jan. 20, http://www.talktalk.co.uk/technology/news/reuters/2006/01/20/onlineattackscommonforbusinesses-fbi.html (current Jan. 14, 2011).

Robbins, J.S. (2002) "The Jihad Online", *National Review,* July 30, http://www.nationalreview.com/robbins/robbins073002.asp (current Jan. 14, 2011).

Robertson, N. and P. Cruickshank (2009) "Recruits Reveal al Qaeda's Sprawling Web, *CNN.com,* July 31, http://www.cnn.com/2009/CRIME/07/30/robertson.al.qaeda.full/index.html (current Jan. 14, 2011).

Ronfeldt, D. and J. Arquilla (2001) "What's Next for Networks and Netwars?" in Arquilla, J. and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica, CA: Rand, pp. 311–361.

Rouleau, E. (2001) "Politics in the Name of the Prophet", *Le Monde Diplomatique,* Nov., http://mondediplo.com/2001/11/09prophet?var_s=rouleau (current Jan. 14, 2011).

Schachtman, N. (2008) "CIA: Hackers Shook Up Power Grids", Jan. 19, http://www.wired.com/dangerroom/2008/01/hackers-take-do/ (current Mar. 3, 2011).

Schmitt, E. and E. Lipton (2010) "Focus on Internet Imams as al Qaeda Recruiters", *New York Times,* Jan. 1, p. A14.

Schultz, E. (2002) "Security Views: Honeypots Make Headlines", *Computers & Security* (21)6, pp. 481–490.

Sewell, W.H. (1992) "A Theory of Structure: Duality, Agency and Transformation", *American Journal of Sociology* (98)1, pp. 1–29.

Shane, S. and A.W. Lehren (2010) "Leaked Cables Offer Raw Look at U.S. Diplomacy", *New York Times,* Nov. 29, p. A1.

Shipley, G. (2010) "Epic Fail: We're Spending Billions on Defenses That Are No Match for the Attacks Skilled Adversaries Are Raining Down on Us. What Can Be Done?" *InformationWeek* (1)282, Oct. 11, pp. 26–38.

Standage, T. (1998) *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*, New York: Walker and Company.

Stern, J. (2002) *Terror in the Name of God: Why Religious Militants Kill*, New York, NY: HarperCollins.

Stern, J. (2003) "The Protean Enemy", *Foreign Affairs,* July–Aug.

Stewart, T.A. (2001) "Six Degrees of Mohamed Atta", *Business 2.0* (2)10, Dec., p. 63.

Stone, B. (2005) "Plain Text: Heroes or Nettlesome Hacks? Some Internet Vigilantes Think They're Fighting Terrorism, But Their Efforts to Shut Down Web Sites Linked to al Qaeda and Other Groups May Be Doing More Harm Than Good", *Newsweek,* July 30, http://www.newsweek.com/2005/07/12/plain-text-heroes-or-nettlesome-hacks.html (current Jan. 14, 2011).

Stone, B. (2009) "As Phones Do More, They Become Targets of Hacking", *The New York Times,* Dec. 21, p. B3.

Sullivan, Laura (2004) "FBI Ties Internet Scam Increase to Organized Crime, Terrorist Sympathizers", *Baltimore Sun,* Feb. 13, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/02/16/BUGSP515731.DTL&type=business (current Jan. 14, 2011).

Symantec (2010) *Symantec Global Internet Security Threat Report: Trends for 2009*, *Vol. XV,* Apr., http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (current Feb.24, 2011).

Tanase, M. (2003) *IP Spoofing: An Introduction,* Mar. 11, http://www.symantec.com/connect/articles/ip-spoofing-introduction (current Jan. 14, 2011).

Tate, R. (2010) *Apple's Worst Security Breach: 114,000 iPad Owners Exposed,* June 9, http://gawker.com/5559346/ (current Jan. 14, 2011).

The Open Source Initiative (2009) *The Open Source Definition*, Open Source Initiative. http://www.opensource.org/docs/osd (current Feb. 24, 2011).

Thomas, T.L. (2003) "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters* (33)1, pp. 112–123.

Thompson, G. (2010) "Early Struggles of Soldier Charged in Leak Case", *The New York Times,* Aug. 9, p. A1.

United Press International (2010) "U.S. Issues No-Read Order on Papers", Dec. 5, http://www.upi.com/Top_News/US/2010/12/05/US-issues-no-read-order-on-leaked-papers/UPI-80221291569329/ (current Jan. 14, 2011).

U.S. Department of Energy (2009) *Smart Grid System Report*, July, http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf (current Jan. 14, 2011).

U.S. Department of Justice (2003) *Southern California Man Who Hijacked Al Jazeera Website Agrees to Plead Guilty to Federal Charges,* Release No. 03-089, June 12, http://www.justice.gov/criminal/cybercrime/racinePlea.htm (current Jan. 14, 2011).

U.S. Government Accountability Office (2010) *Testimony Before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives. Information Security: Concerted Response Needed to Resolve Persistent Weaknesses,* Mar. 24, http://www.gao.gov/new.items/d10536t.pdf (current Jan. 13, 2011).

USAToday.com (2002) "Experts: Islamic Hackers Ready for Cyber War", Oct. 29, http://www.usatoday.com/tech/news/computersecurity/2002-10-29-cyber-attacks_x.htm (current Jan. 14, 2011).

Vamosi, R. (2005) "Alarm over 'Pharming' Attacks", *Cnet.com,* Feb. 18, http://reviews.cnet.com/4520-3513_7-5670780-1.html (current Jan. 14, 2011).

Verton, D. (2003) *Black Ice: The Invisible Threat of Cyber-Terrorism*, Emeryville, CA: McGraw-Hill Osborne.

Walton, M. (2005) "New Computer Scam Holds Your Info for Ransom: 'Trojan' Encrypts Files, Demands $200 for Key", *CNN.com*, May 25, http://www.cnn.com/2005/TECH/internet/05/25/ransomware/index.html (current Jan. 14, 2011).

Warden, J.A. (1994) Air Theory for the Twenty-first Century. In K.P. Magyar et al. (eds.) *Challenge and Response*. Maxwell AFB, AL: Air University Press, pp. 311–332.

Weston, G. (2011) "Foreign Hackers Attack Canadian Government: Computer Systems at 3 Key Departments Penetrated", *CBC.ca*, Feb. 16, http://www.cbc.ca/news/technology/story/2011/02/16/pol-weston-hacking.html (current Mar 3, 2011).

Wired (2003) "War Hack Attacks Tit for Tat", Mar. 28, http://www.wired.com/politics/law/news/2003/03/58275 (current Jan. 14, 2011).

Wired (2004) "Expert: Microsoft Dominance Poses Security Threat", Feb. 15, http://www.wired.com/politics/security/news/2004/02/62307 (current Jan. 14, 2011).

Zack, M.H. (1993) "Interactivity and Communication Mode Choice in Ongoing Management Groups", *Information Systems Research* (4)3, pp. 207–239.

Zanini, M. and S.J.A. Edwards (2001) “The Networking of Terror in the Information Age” in Arquilla, J. and D. Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica, CA: Rand: pp. 29–60.

ABOUT THE AUTHORS

Wm. David Salisbury (Ph. D., University of Calgary, 1996) is an Associate Professor with the Department of MIS, OM & Decision Sciences at the University of Dayton. Dave investigates organizational impacts of information technology, particularly the influence of computer-mediated communication on group interaction and how technology is used to store and transmit organizational knowledge. He has also co-authored papers featuring the use of structural equation modeling for confirmatory factor analysis in survey measurement development, and more recently a paper on how Internet information intermediaries may influence offered and transacted prices. His work has been published in *Information Systems Research, Small Group Research*, *Information & Management*, *Decision Support Systems*, *The Communications of the Association for Information Systems*, *The Database for Advances in Information Systems*, and *Electronic Markets*. Dave is also currently a Senior Editor at *The Database for Advances in Information Systems*.

David W. Miller (Ph.D. Mississippi State University, 2003) is an Associate Professor in the Accounting and Information Systems Department at California State University, Northridge. In addition to a Ph.D. in business information systems, he has a BSBA in management, an MBA emphasizing economics, and an MSBA in information systems, all from Mississippi State University. His research interests are in areas of social impacts of information systems on groups and organizations, technology adoption and use, managing information security, and awareness and impacts in social networking. Dr. Miller teaches a variety of courses at the undergraduate and graduate level in subjects ranging from the role and impact of information systems in business as well as management of information security. He has twice earned the departmental IS Professor of the Year award.

Jason M. Turner (Ph.D., University of Texas at Austin, 2006) is a lieutenant colonel in the United States Air Force and currently serves as the Professor of Aerospace Studies at Indiana University, Bloomington. He holds a Ph.D. in information science, an MS in information resource management, and professional certifications in Usability Analysis and Enterprise Architecture. As a cyber operations officer, Dr. Turner has held a variety of positions providing fixed-based and deployed/tactical technology services and oversight. In one such assignment he helped to develop nation-wide data and voice network, radio and satellite communications capabilities for US and Coalition personnel stationed throughout Afghanistan and Pakistan. Dr. Turner has taught resident and online graduate and undergraduate-level courses in leadership and management; national and regional studies; research methods; data communications and networking; usability and interface design; information and database systems analysis, design, and management; knowledge management; and other information, technology, and systems-related topics. His research interests include psychological, social, and organizational impacts and uses of information and information technology.